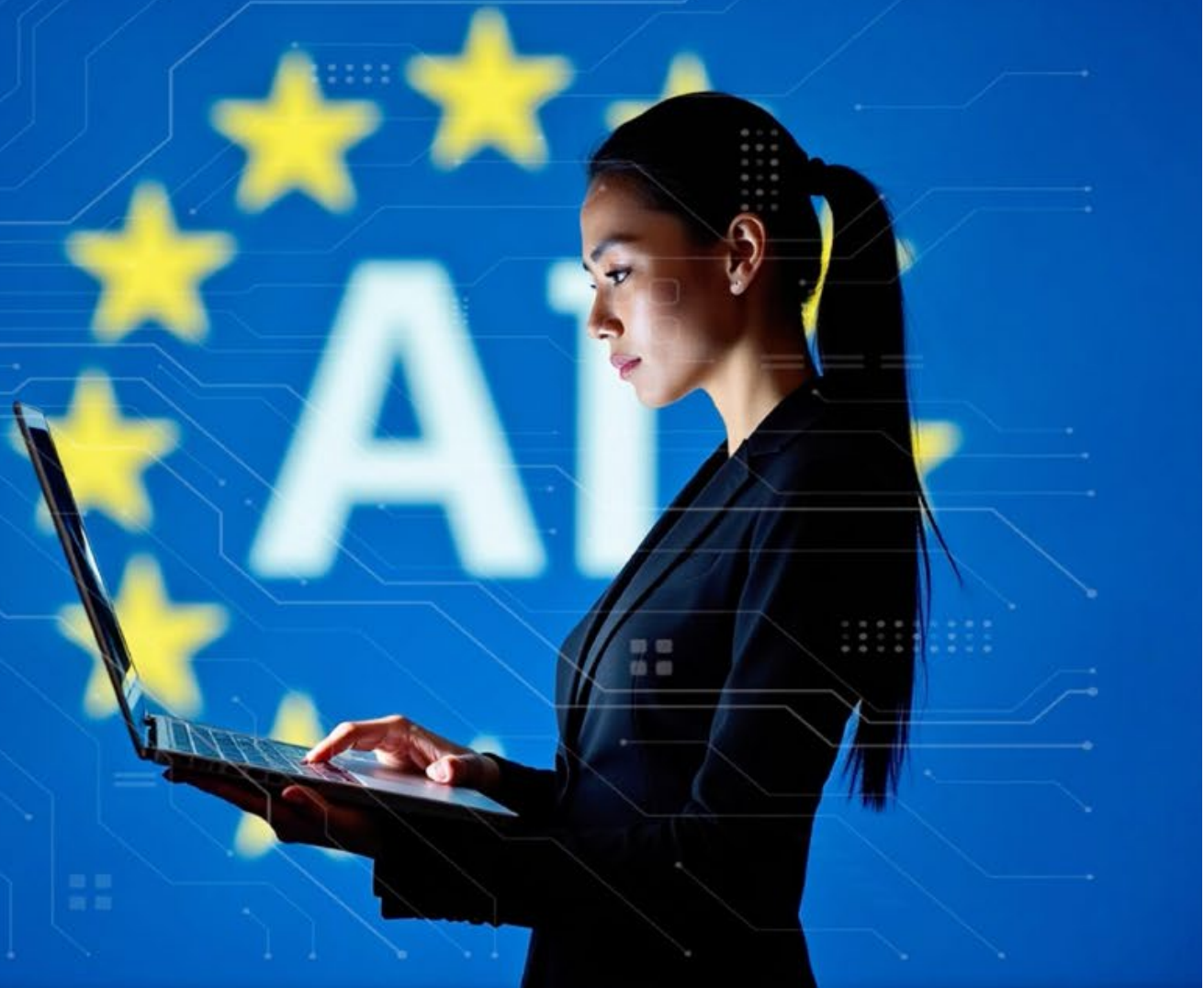
REGOLAMENTO EUROPEO SULL'INTELLIGENZA ARTIFICIALE

2024/1689

AI COMPLIANCE:
QUELLO CHE LE AZIENDE DEVONO SAPERE PRIMA DI USARE L'INTELLIGENZA ARTIFICIALE

AVVERA | SB Società Benefit



AGENDA

AVVERA | SB Società Benefit

- I principi alla base e gli obiettivi del Regolamento
- Fasi di attuazione e termini da rispettare
- Ruoli, obblighi e responsabilità
- Classificazione dei rischi e conseguenze pratiche
- Come mitigare il rischio per evitare le sanzioni
- Approcci per una gestione agile ed efficace

generated by human®

AVVERA

PERCHÉ SI PARLA DI AI?

Queste tecnologie oggi stanno avendo un forte impatto nelle nostre vite. 2 fattori:

- Crescita esponenziale della **capacità di calcolo dei computer;**
- Con la diffusione dell'utilizzo dei pc, poi di internet e oggi degli smartphone abbiamo prodotto un volume sempre più grande di dati: **«i Big Data sono il petrolio per far funzionare i motori dei sistemi di AI».**

AVVERA

L'AI NELLE AZIENDE ITALIANE

Secondo lo studio "AI Radar" pubblicato da Boston Consulting Group (BCG) in occasione del World Economic Forum di Davos, è emerso che siamo tra i paesi più arretrati per formazione dei dipendenti in materia di AI/Generative AI, con solo il 20% delle aziende che ha formato almeno un quarto dei dipendenti.

Il vero rischio è che il lavoro venga "rubato" da altre aziende che opereranno con persone che utilizzano con grande efficacia sistemi AI.

AVVERA

REGOLAMENTO (UE) 2024/1689

Il 1° agosto è entrato ufficialmente in vigore il Regolamento sull' AI dell'UE (AI Act), con l'obbiettivo di promuovere uno sviluppo e un'implementazione responsabile dell'AI in tutta l'Europa.

Il regolamento dell'UE sull'intelligenza artificiale è il primo atto legislativo al mondo a disciplinare la materia: definisce e armonizza i principi applicabili alla diffusione delle tecnologie basate su intelligenza artificiale, allineandosi ai valori e ai diritti fondamentali cardine della visione europea.

AVVERA

GLI SCOPI DEL REGOLAMENTO

1. **migliorare il funzionamento del mercato interno**, istituendo un quadro giuridico uniforme per quanto riguarda lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di intelligenza artificiale nell'Unione, in conformità dei valori dell'Unione;
2. promuovere la diffusione di un'intelligenza artificiale (IA) **antropocentrica e affidabile;**
3. garantire un livello **elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea**, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente;
4. proteggere contro gli **effetti nocivi** dei sistemi di IA nell'Unione;
5. **promuovere l'innovazione**.

1

AVVERA | SB Società Benefit

PERCHÉ UNA REGOLAMENTAZIONE SULL'AI?

AVVERA SRL SB

AMBITO DI APPLICAZIONE

Art. 3 AI Act

Le norme contenute nel Regolamento si applicano ai sistemi e ai modelli che presentano determinate caratteristiche:

«**sistema di intelligenza artificiale**»: “**sistema automatizzato** progettato per funzionare con **livelli di autonomia variabili** e che può presentare **adattabilità** dopo la diffusione e che, per obiettivi espliciti o impliciti, **deduce dall'input che riceve come generare output** quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali”.

«**modello di intelligenza artificiale**»: “addestrato con grandi quantità di dati utilizzando l'autosupervisione su larga scala, che sia caratterizzato una generalità significativa e sia in grado di svolgere con competenza un'ampia gamma di compiti distinti, indipendentemente dalle modalità con cui il modello è immesso sul mercato, e che può essere integrato in una varietà di sistemi o applicazioni a valle”.

AVVERA

CHE COS'È L'INTELLIGENZA ARTIFICIALE

- **L'Intelligenza Artificiale (IA)** è una disciplina dell'informatica che studia lo sviluppo dei sistemi hardware e software dotati di capacità tipiche dell'essere umano (apprendimento, interazione con l'ambiente, adattamento, ragionamento e pianificazione).

- **Il Machine Learning (ML)** è una **sottocategoria dell'IA** che si concentra sulla capacità delle macchine di imparare dai dati.

- Attraverso l'analisi di grandi volumi di dati, questi sistemi sono in grado di apprendere pattern e correlazioni, migliorando le loro prestazioni nel tempo e senza essere esplicitamente programmati con regole specifiche per ogni possibile soluzione.

L’ AI NELLA SOCIETÀ

L’ AI non è un prodotto. È una attivatore di molte industrie e ambiti della vita umana: ricerca scientifica, istruzione, manifattura, logistica, trasporti, difesa, arte e molto altro ancora.

Industria manifatturiera

L’IA razionalizza i processi, ottimizza le risorse, aumenta la produttività e riduce l’impatto ambientale delle imprese

Sicurezza

Un’analisi predittiva e una gestione dei rischi migliori contribuiscono a prevenire gli incidenti o a ridurne l’impatto

Istruzione

L’IA consente un apprendimento personalizzato, migliorando la partecipazione ei risultati. Automatizza i compiti amministrativi degli insegnanti, consentendo loro di dedicare più tempo a insegnamento e tutoraggio

https://www.consilium.europa.eu/it/policies/ai-explained/

L' AI NELLA SOCIETÀ

Assistenza sanitaria

I prestatori di assistenza sanitaria utilizzano l'IA per migliorare la diagnostica, prevedere le malattie e personalizzare i trattamenti, il che si traduce in un'assistenza e i risultati migliori per i pazienti

Energia

L'IA rende la produzione e l'uso di energie più efficienti e sostenibili, riducendo le emissioni di gas a effetto serra e contrastando i cambiamenti climatici

Trasporti

I veicoli autonomi funzionano in modo sicuro senza l'intervento umano. L'IA ottimizza inoltre la gestione del traffico e prevede le esigenze di manutenzione delle infrastrutture

https://www.consilium.europa.eu/it/policies/ai-explained/

AVVERA

COME FUNZIONA L'AI?

Il Machine Learning si concentra sullo sviluppo di programmi in grado di apprendere dai dati:

4 fasi:

1. Raccolta;
2. Addestramento;
3. Validazione;
4. Utilizzo.

AVVERA

COME FUNZIONA L'AI?

Un algoritmo nel contesto del machine learning è una sequenza di istruzioni matematiche e logiche che guida un sistema nell'apprendimento dei dati.

È il metodo o la procedura utilizzata per analizzare i dati e apprendere ai pattern presenti in essi. Es. le reti neurali.

Grazie ai dati e agli algoritmi siamo in grado di generare un **modello.** Un modello di AI è un'entità matematica, che è stata addestrata su un insieme di dati per fare previsioni o riconoscere pattern.

USO RESPONSABILE DELL'AI

- Sfida sul piano della privacy e della sicurezza:

- È essenziale dare priorità a un utilizzo sicuro degli strumenti di AI generativa – proteggere le informazioni sensibili (personali, dei propri clienti e della propria azienda) è di fondamentale importanza.

- Dobbiamo farne un uso etico, basato sulla tutela dei dati.

- Licenze con strumenti di AI: non condividere dati personali sensibili.

2

AVVERA | SB Società Benefit

FASI DI ATTUAZIONE E TERMINI DA RISPETTARE

AVVERA

FASI DI ATTUAZIONE

Entrato in vigore il 2 agosto 2024, l'AI Act prevede **un'applicazione graduale delle sue disposizioni** e si applicherà dal **2 agosto 2026:**

Il **2 febbraio 2025** diventano operative due gruppi di disposizioni chiave:

- I divieti relativi a determinate pratiche di AI (art. 5)
- I requisiti in materia di Alfabetizzazione in materia di AI (art. 4)

Il **2 agosto 2025: capo III, sezione 4** (autorità di notifica designate dagli stati membri), il **capo V** (modelli di AI per finalità generali), il **capo VII** (banca dati UE per i sistemi ad alto rischio), il **capo XII** (sanzioni) e l'**art. 78** (riservatezza dei dati trattati in conformità al regolamento , ad eccezione dell'art. 101 (Sanzioni pecuniarie per i fornitori di modelli di IA per finalità generali);

AVVERA

FASI DI ATTUAZIONE

Il **2 agosto 2027**: **art. 6, paragrafo 1** (classificazione dei sistemi ad alto rischio), e i corrispondenti obblighi di cui al Regolamento.

Inoltre, l'AI Act richiama diversi documenti pensati per fornire delle indicazioni più di dettaglio rispetto alle disposizioni del Regolamento, es. l'art. 56 dell'AI Act, è stata pubblicata la prima bozza del "**Codice di buone pratiche**" relativo ai modelli di IA per finalità generali e ai modelli di IA per finalità generali con rischio sistemico. il Codice sarà pronto al più tardi entro il **2 maggio 2025.**

Per la timeline completa:

https://artificialintelligenceact.eu/implementation-timeline/?utm_source=substack&utm_medium=email

AVVERA

ALFABETIZZAZIONE

Art. 4. ruolo cruciale dell'alfabetizzazione IA nella tutela dei diritti fondamentali, della salute e della sicurezza dei cittadini.

Il regolamento introduce un obbligo specifico di garantire un adeguato livello di alfabetizzazione all'AI per il personale coinvolto nell'utilizzo dei sistemi di AI: l'obbligo prevede che i fornitori e gli utilizzatori (deployer) di AI adottino misure per garantire che il personale rilevante (inclusi i fornitori) che usa l'IA abbia un "livello sufficiente di alfabetizzazione all'IA", tenendo conto del contesto e delle persone potenzialmente interessate dal sistema di AI in uso.

Non sono previste sanzioni in caso di mancato rispetto della prescrizione ma nell'ipotesi di incidenti, malfunzionamenti o conseguenze negative ne potrebbero derivare responsabilità giuridiche, assicurative e reputazionali.

AVVERA

ALFABETIZZAZIONE

L’AI Office ha creato un «archivio vivente» di pratiche di alfabetizzazione, per tenere conto delle diverse specificità delle organizzazioni e fornire esempi pratici da cui trarre inspirazione. In generale raccomandano di agire su tre fronti formativi:

- **Momenti collettivi volti allo sviluppo delle conoscenze fattuali sull’IA e le sue applicazioni**, attraverso lo studio e l’esperienza diretta. A riguardo, è possibile predisporre workshop e veicolare, all’interno dell’organizzazione, linee guida e best practices di settore.
- **Focus sui rischi legati all’IA e sul perché delle decisioni**. Infatti, è necessario comprendere il “perché” delle sue decisioni, così da intercettarne gli errori e i malfunzionamenti. Lo sviluppo di tali conoscenze include, ma non è limitato a, la comprensione di che cosa è l’IA, anche nel contesto organizzativo, e di quali sono i rischi che essa comporta.
- **Revisione interna di linee guida e policy ad hoc**. Per sviluppare le competenze necessarie, si suggerisce di applicare le informazioni fattuali raccolte in materia di IA nella quotidianità, sia professionale sia personale. A tal fine, può rivelarsi utile organizzare workshop e interventi formativi volti ad analizzare casi studio su dilemmi etici legati all’IA e incentivare il processo di revisione interna di linee guida e altri strumenti di policy affinché risultino chiari ed esaustivi.

3

AVVERA | SB Società Benefit

RUOLI OBBLIGHI E RESPONSABILITÀ

AVVERA SRL SB

AVVERA

A CHI SI RIVOLGONO LE REGOLE?

Buona parte del Regolamento è indirizzato ad aziende (“**Provider**”) che sviluppano e forniscono sistemi AI; tuttavia, i requisiti principali si applicano a chiunque utilizzi (“**Deployer**”) sistemi AI, in quanto, in molte situazioni, **è lo scopo dell’utilizzo che ne determina i possibili impatti e rischi.**

Fornitore

una persona fisica o giuridica, un’autorità pubblica, un’agenzia o un altro organismo che **sviluppa** un sistema di IA o un modello di IA per finalità generali **o che fa sviluppare** un sistema di IA o un modello di IA per finalità generali **e immette tale sistema o modello sul mercato o mette in servizio il sistema di IA con il proprio nome o marchio**, a titolo oneroso o gratuito.

Deployer

la persona fisica o giuridica, autorità pubblica, agenzia o altri organismi **che utilizzano un sistema di IA sotto la propria autorità**, ad **eccezione** nel caso in cui il sistema di IA sia utilizzato nel corso di **un’attività personale non professionale**.

AVVERA

GLI OBBLIGHI

- **Una delle caratteristiche più innovative dell'AI Act è l'introduzione di obblighi specifici in base ad un approccio basato sul rischio per la regolamentazione dei sistemi di AI:**

- **Rischi minimi o nulli:** la maggior parte dei sistemi di IA non pone rischi. Videogiochi o i filtri antispam basati sull'IA possono essere utilizzati liberamente. **Non sono disciplinati** o interessati dal Regolamento, anche se le imprese sono incoraggiate ad adottare volontariamente codici di condotta.

- **Rischi limitati**: i sistemi di IA che presentano solo rischi limitati, come chatbot o sistemi di IA che generano contenuti, sono soggetti a **obblighi di trasparenza**, come l'obbligo di informare gli utenti che i contenuti sono generati ricorrendo all'IA, in modo che possano prendere decisioni informate in merito all'ulteriore utilizzo.

- **Rischi elevati**: I sistemi di IA ad alto rischio, come quelli utilizzati nella diagnosi delle malattie, nella guida autonoma e nell'identificazione biometrica delle persone coinvolte in attività criminali o indagini penali, devono soddisfare **requisiti e obblighi rigorosi per accedere al mercato dell'UE**. Tali requisiti e obblighi comprendono **test rigorosi, garanzia di alta qualità dei dati utilizzati, trasparenza e supervisione umana, livelli adeguati di accuratezza, robustezza e sicurezza**

- **Rischi inaccettabili: nell'UE è vietato l'utilizzo** dei sistemi che rappresentano una minaccia per la sicurezza, i diritti o i mezzi di sussistenza delle persone come quelli che permettono il «social scoring» da parte di governi o manipolano il comportamento umano in modo dannoso.

AVVERA

I NUOVI RUOLI IN AZIENDA

L'articolo 28 del Regolamento introduce l'obbligo, per i fornitori di sistemi di intelligenza artificiale ad alto rischio, di designare un **AI Compliance Officer,** sarà il punto di riferimento per tutte le questioni relative alla conformità dei sistemi di intelligenza artificiale utilizzati dall'azienda. Un ruolo che richiede competenze interdisciplinari, a cavallo tra diritto, tecnologia ed etica, e che dovrà garantire il rispetto degli obblighi previsti dal Regolamento

L'articolo 17 del Regolamento introduce **il Responsabile del sistema di gestione qualità**. Un ruolo fondamentale per garantire che i sistemi di intelligenza artificiale ad alto rischio siano sviluppati, implementati e monitorati secondo standard qualitativi adeguati.

L'articolo 57 del Regolamento prevede l'istituzione di un **Comitato Etico**, obbligatorio per gli enti pubblici e le grandi imprese. Un organo collegiale con composizione multidisciplinare, che dovrà includere giuristi, tecnici e persino filosofi. Il Comitato Etico avrà il compito di valutare le implicazioni etiche dei sistemi di intelligenza artificiale utilizzati dall'azienda, garantendo **che il loro sviluppo e utilizzo avvenga nel rispetto dei diritti fondamentali e dei valori europei**. Un ruolo che va oltre la mera conformità normativa.

AVVERA

GLI ALTRI RUOLI

Rappresentante autorizzato

una persona fisica o giuridica ubicata o stabilita nell'Unione che ha **ricevuto e accettato un mandato scritto da un fornitore** di un sistema di IA o di un modello di IA per finalità generali al fine, rispettivamente, di adempiere ed eseguire per suo conto gli obblighi e le procedure stabiliti nel presente regolamento.

Importatore

una persona fisica o giuridica ubicata o stabilita nell'Unione che immette sul mercato un sistema di IA **recante il nome o il marchio di una persona fisica o giuridica stabilita in un paese terzo.**

Distributore

una persona fisica o giuridica nella catena di approvvigionamento diversa dal fornitore o dall'importatore, che mette a disposizione un sistema di IA sul mercato dell'Unione.

AVVERA

GOVERNANCE E SUPERVISIONE

Per garantire la conformità e un'applicazione efficace delle regole, l' Ai Act prevede la creazione di un sistema di governance multilivello, con autorità a livello nazionale e a livello europeo:

A livello europeo:

- un **Ufficio AI all'interno della Commissione** per far rispettare le regole comuni in tutta l'UE
- un **gruppo scientifico di esperti indipendenti** per sostenere le attività di esecuzione.
- un **comitato per l'AI** composto da rappresentanti degli Stati membri e incaricato di fornire consulenza e assistenza alla Commissione e agli Stati membri ai fini di un'applicazione coerente ed efficace del regolamento sull'IA.
- un **forum consultivo** per i portatori di interessi volto a fornire competenze tecniche al comitato per l'IA e alla Commissione.

AVVERA

GOVERNANCE E SUPERVISIONE

A livello nazionale:

Per **autorità di notifica** si intende il soggetto istituzionale nazionale competente, nel gestire, monitorare e vigilare tutta la fase di certificazione dei sistemi di intelligenza artificiale.

L'autorità di vigilanza ha il compito di controllare che l'AI Act sia rispettato da parte di produttori e distributori dei sistemi di AI attraverso poteri di indagine e in grado di sanzionare pecuniariamente le violazioni.

In tale contesto in **Italia**, con una legge ora in fase di approvazione in parlamento, si attribuiscono le funzioni di vigilanza all'**Agenzia nazionale per la cybersicurezza**, mentre le funzioni di notifica all'**Agenzia per l'Italia digitale.**

AVVERA

SANZIONI

Struttura su tre livelli:

i. **fino a 35 milioni di euro o al 7% del fatturato mondiale totale annuo dell'esercizio precedente (se superiore)** per violazioni relative a pratiche vietate o per l'inosservanza di requisiti in materia di dati;
ii. **fino a 15 milioni di euro o al 3% del fatturato mondiale totale annuo dell'esercizio precedente** per l'inosservanza di qualsiasi altro requisito o obbligo del regolamento**;**
iii. **fino a 7,5 milioni di euro o all'1,5% del fatturato mondiale totale annuo dell'esercizio precedente** per la fornitura di informazioni inesatte, incomplete o fuorvianti agli organismi notificati e alle autorità nazionali competenti in risposta a una richiesta.

L'importo delle sanzioni è calcolato sulla base di una percentuale del fatturato complessivo realizzato dalla società nell'anno precedente o su un importo fisso, se superiore. Le PMI e le start-up sono soggette a sanzioni pecuniarie proporzionali.

4

AVVERA | SB Società Benefit

CLASSIFICAZIONE DEI RISCHI E CONSEGUENZE PRATICHE

5

AVVERA | SB Società Benefit

RISCHIO INACCETTABILE

I SISTEMI A RISCHIO INACCETTABILE (ART. 5)

Divieto di utilizzo:

- **Tecniche subliminali, manipolative,** ingannevoli per distorcere materialmente il comportamento e compromettere il processo decisionale informato, causando un danno significativo; es. nel marketing il c.d. “nudging”
- **sfruttamento di vulnerabilità legate all’età, alla disabilità o alle condizioni** socioeconomiche per distorcere in modo marziale il comportamento, causando (con ragionevole probabilità) un danno significativo;
- **social scoring,** ossia la valutazione o la classificazione di individui o gruppi in base al comportamento sociale o alle caratteristiche personali, causando un trattamento negativo o sfavorevole di tali persone.
- **Valutazione del rischio che un individuo commetta reati (l’uso dell’AI per la polizia predittiva)** basata sulla profilazione e i sistemi che utilizzano dati biometrici per classificare le persone in base a categorie specifiche come razza, religione o orientamento sessuale.
- sistemi di IA che **creano o ampliano le banche dati di riconoscimento facciale mediante scraping** non mirato di immagini facciali da internet o da filmati di telecamere a circuito chiuso.

I SISTEMI A RISCHIO INACCETTABILE (ART. 5)

- i sistemi di IA per **inferire le emozioni di una persona fisica nell'ambito del luogo di lavoro e degli istituti di istruzione** (tranne dove l'uso del sistema di IA sia destinato a essere messo in funzione o immesso sul mercato per motivi medici o di sicurezza).
- L'uso di sistemi di **identificazione biometrica remota in tempo reale (RBI) in spazi accessibili al pubblico a fini di attività di contrasto**, **a meno che**, e nella misura in cui, tale uso sia strettamente necessario per:

  1) la **ricerca mirata di specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale di esseri umani,** nonché la ricerca di persone scomparse;

  2) la prevenzione di una **minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche** o di una minaccia reale e attuale o reale e prevedibile di un attacco terroristico;

  3) la **localizzazione o l'identificazione di una persona sospettata di aver commesso un reato**, ai fini dello svolgimento di **un'indagine penale**, o dell'esercizio di un'azione penale o dell'esecuzione di una sanzione penale per i reati di cui all'allegato II del Regolamento, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno quattro anni.

6

AVVERA

SB

Società Benefit

RISCHIO ALTO

AVVERA

I SISTEMI AD ALTO RISCHIO

I sistemi di IA ad alto rischio sono sottoposti a obblighi di conformità tecnica e valutazione di impatto (art. 17,27)

Caratteristiche:

1. **impatto significativo**: possono influenzare decisioni critiche che riguardano la vita, la salute, la sicurezza o i diritti fondamentali **delle persone.**
2. **Settori critici**: operano in settori considerati sensibili come sanità, trasporti, energia, educazione, gestione delle risorse umane e sistemi di sicurezza.

AVVERA

I SISTEMI AD ALTO RISCHIO

Art.6, paragrafo 1, del Regolamento, un sistema di IA è considerato ad alto rischio se soddisfa due condizioni principali:

1. **utilizzo come componente di sicurezza**: il sistema è impiegato come componente di un prodotto regolato dalla normativa europea, come nel caso delle direttive sulla sicurezza dei giocattoli o degli ascensori
2. **valutazione di conformità**: il prodotto che incorpora il sistema di IA deve essere soggetto a una valutazione da parte di terzi prima della sua immissione sul mercato o della sua messa in servizio ai sensi della normativa di armonizzazione dell'Unione elencata nell'Allegato I

Inoltre, l'Allegato III del Regolamento (art.6, paragrafo 2) elenca i settori specifici in cui i sistemi di IA sono considerati ad alto rischio:

AVVERA

I SISTEMI AD ALTO RISCHIO

- **Sistemi di IA utilizzati per l'identificazione biometrica remota**, il riconoscimento delle emozioni e la categorizzazione biometrica (ad esempio un sistema di IA per identificare retroattivamente un taccheggiatore)
- Componenti di sicurezza dell'IA nelle **infrastrutture critiche** (ad esempio i trasporti), il cui guasto potrebbe mettere a rischio la vita e la salute dei cittadini
- Soluzioni di IA utilizzate negli **istituti di istruzione**, che possono determinare l'accesso all'istruzione e il corso della vita professionale di una persona (ad esempio il punteggio degli esami)
- Strumenti di IA **per l'occupazione, la gestione dei lavoratori e l'accesso al lavoro autonomo** (ad esempio software di selezione dei CV per l'assunzione)
- Alcuni casi d'uso dell'IA **utilizzati per dare accesso a servizi pubblici e privati essenziali** (ad esempio il credit scoring che nega ai cittadini l'opportunità di ottenere un prestito)
- Casi d'uso dell'IA nelle **attività di contrasto** che possono interferire con i diritti fondamentali delle persone (ad esempio valutazione dell'affidabilità delle prove)
- Casi d'uso dell'IA nella **gestione della migrazione, dell'asilo e del controllo delle frontiere (ad esempio esame automatizzato delle domande di visto)**
- Soluzioni di IA utilizzate **nell'amministrazione della giustizia e dei processi democratici** (ad esempio soluzioni di IA per preparare le sentenze dei tribunali)

7

AVVERA | SB Società Benefit

RISCHIO LIMITATO

AVVERA SRL SB

AVVERA

SISTEMI A RISCHIO LIMITATO

Questi sistemi sono soggetti ad **obblighi di trasparenza:** I contenuti generati dall'intelligenza artificiale dovranno quindi essere identificati come tali in maniera agevole, permettendo quindi ai soggetti esposti di prendere decisioni informate e adottare le misure di cautela necessarie:

Caratteristiche:

1. Interazione diretta con gli esseri umani.
2. Potenziale di influenzare il comportamento o le decisioni delle persone.

Esempi di sistemi a rischio limitato:

1. Chatbot e assistenti virtuali;
2. Sistemi di AI che generano o manipolano contenuti audio o video (es. deepfake)
3. sistemi di AI utilizzati per la personalizzazione dei contenuti sui social media.

8

AVVERA | SB Società Benefit

RISCHIO MINIMO

AVVERA SRL SB

AVVERA

SISTEMI A RISCHIO MINIMO

La maggior parte dei sistemi di IA rientra in questa categoria e non è soggetta a obblighi specifici previsti dal Regolamento, ma dovranno comunque rispondere ai requisiti previsti dal Regolamento Generale per la Protezione dei Dati (Regolamento 2016/679/UE), dalla Direttiva Copyright (Direttiva 2019/790/UE), dalla Direttiva sulla responsabilità da prodotto difettoso (adottata in seduta plenaria il 12 marzo 2024, per l'aggiornamento della Direttiva 85/374/CEE) e delle **specifiche normative di settore.**

Caratteristiche dei sistemi a rischio minimo:

1. Basso o nessun rischio per i diritti o la sicurezza delle persone.
2. Utilizzo in applicazioni non sensibili o in contesti ben controllati.

Esempi di sistemi a rischio minimo:

1. Filtri spam nelle email;
2. Sistemi di AI utilizzati nei videogiochi;
3. Sistemi di raccomandazione per prodotti in un e-commerce (con alcune eccezioni);
4. Sistemi di AI utilizzati per l'ottimizzazione dei processi industriali.

9

AVVERA | SB Società Benefit

CONSEGUENZE PRATICHE

OBBLIGHI PER I SISTEMI AD ALTO RISCHIO

- Art. 16 AI Act
- **Per i sistemi di IA ad alto rischio, il Regolamento prevede una serie di requisiti specifici da rispettare prima della loro immissione sul mercato:**
- La conformità di un sistema di IA ad alto rischio è valutata in relazione ai requisiti previsti dalla Sezione 2 (« Requisiti per i sistemi di IA ad alto rischio ») del Capo III, artt. 8 e ss. del Regolamento sull'IA:
- In particolare, tra questi requisiti è ricompreso un sistema di gestione del rischio (art. 9), set di dati di addestramento, convalida e prova secondo criteri di qualità`, pratiche di governance e gestione dei dati adeguate alla finalità (art. 10), la redazione di una documentazione tecnica (art. 11), la registrazione automatica degli eventi (« log ») durante il loro funzionamento (art. 12), la trasparenza e fornitura di informazioni ai deployer (art. 13), la sorveglianza umana (art. 14), l'accuratezza, robustezza e cibersicurezza (art. 15)

LA CONFORMITÀ A LIVELLO EUROPEO

- Per agevolare questo processo, la Commissione Europea si baserà su standard proposti da enti di normazione come l'Organizzazione Internazionale per la Standardizzazione (ISO) e il Comitato Europeo di Normazione (CEN), che forniranno un quadro di riferimento per valutare la conformità dei sistemi AI e garantire un approccio coerente e uniforme nell'intera Unione Europea.

MECCANISMI DI CONTROLLO DELLA CONFORMITÀ

Per garantire la conformità e l'applicazione delle regole, l'AI Act introduce meccanismi di controllo.

- **Valutazione della conformità:** può essere effettuata **internamente o da organismi notificati**, a seconda del tipo di sistema; Per i sistemi non ad alto rischio, **auto-valutazione della conformità da parte del fornitore**.
- **Registrazione dei sistemi ad alto rischio:** la valutazione deve essere inserita in una **banca dati dell'UE,** prima di immetterli nel mercato; **Marcatura CE** apposta sul sistema di IA ad alto rischio in modo visibile, leggibile e indelebile.
- **Monitoraggio dopo l'immissione sul mercato:** implementare un sistema di monitoraggio per la raccolta e l'analisi dei dati relativi all'uso dei sistemi; Obbligo di **segnalare incidenti gravi o malfunzionamenti alle autorità competenti.**
- **Ispezioni e audit:** Le autorità di vigilanza del mercato possono condurre ispezioni e richiedere l'accesso ai dati, documentazione e codice sorgente; Possibilità di audit da parte di terze parti indipendenti.

AVVERA

MECCANISMI DI CONTROLLO DELLA CONFORMITÀ

- **Misure correttive:**
  Le autorità possono ordinare il ritiro o il richiamo dei sistemi di AI che risultano non essere conformi;
  Possibilità di richiedere modifiche ai sistemi per garantire la conformità.

- **Sanzioni:**
  Gli stati membri devono stabilire regimi sanzionatori efficaci, proporzionati e dissuasivi;
  Le sanzioni possono arrivare fino al 7% del fatturato globale annuo dell'azienda per le violazioni più gravi.

- **Protezione degli informatori:**
  L'AI Act prevede **protezioni per gli individui** che segnalano violazioni alle autorità competenti.

- **Codici di Condotta:**
  Incoraggiamento allo sviluppo di codici di condotta volontari per i fornitori di sistemi di AI non ad alto rischio.

AVVERA

VALUTAZIONE DEL RISCHIO

Secondo i criteri indicati dal Regolamento, la classificazione è basata sulla valutazione dei rischi per i diritti degli individui europei e deve essere fatta in primo luogo dai fornitori dei sistemi AI e può dipendere da:

- **caso d'uso**, ovvero da come il sistema AI è utilizzato in azienda;
- quali **dati** sono elaborati da questo;
- con quali **finalità e modalità** di elaborazione.

AVVERA

SISTEMA DI GESTIONE DEI RISCHI

Art. 9 sistema di gestione dei rischi.

4 fasi:

1. **Identificazione e analisi dei rischi:** Analisi dei potenziali impatti negativi su salute, sicurezza e diritti fondamentali; Considerare rischi specifici del settore in cui il sistema verrà utilizzato.

2. **Stima della probabilità e gravità dei rischi:** Valutazione sulla probabilità che si verifichino scenari di rischio; Stima la gravità dei potenziali danni.

3. **Valutazione delle misure di mitigazione:** Identificazione e implementazione delle misure per mitigare i rischi individuati; Valutazione dell'efficacia delle misure di mitigazione.

4. **Adozione delle misure:** Registrazione del processo di valutazione, delle conclusioni e delle decisioni prese; Implementazione di un sistema di monitoraggio continuo; Aggiornamenti in base ai dati raccolti e all'esperienza operativa.

AVVERA

OBBLIGHI PER IL DEPLOYER

L'art. 26 AI Act introduce gli obblighi a cui è tenuto il deployer dei sistemi di AI ad alto rischio:

- **Misure tecniche e organizzative a garanzia dell'utilizzo dei sistemi**, conformemente alle istruzioni per l'uso fornite dai fornitori;
- **Sorveglianza umana:** persone fisiche che dispongono della competenza, della **formazione** e autorità necessarie;
- **Istruzioni per l'uso e obbligo di informare:** monitorare il funzionamento del sistema di IA ad alto rischio e, se del caso, informare i Informare senza ritardo il fornitore e la pertinente autorità di vigilanza del mercato, sospendere l'uso qualora abbiano motivo di ritenere che l'uso del sistema di AI d alto rischio in conformità delle istruzioni possa presentare **un rischio per la salute, sicurezza o i diritti fondamentali delle persone**; Inoltre, informare immediatamente il fornitore e successivamente l'autorità di vigilanza, qualora abbiano individuato un **incidente grave**.

AVVERA

OBBLIGHI PER IL DEPLOYER

Art. 27 AI Act. Prima di utilizzare un sistema di ad alto rischio, per alcune categorie di deployer (organismi di diritto pubblico o enti privati che forniscono servizi pubblici e i deployer di sistemi di IA ad alto rischio di cui all'allegato III, punto 5, lettere b) e c) (affidabilità creditizia e assicurazioni sulla vita/assicurazioni sanitarie), il Regolamento prevede di **effettuare una valutazione dell'impatto sui diritti fondamentali:**

a) una **descrizione dei processi del deployer** in cui il sistema di IA ad alto rischio sarà utilizzato in linea con la sua finalità prevista;
b) una **descrizione del periodo di tempo** entro il quale ciascun sistema di IA ad alto rischio è destinato a essere utilizzato e con che frequenza;
c) le categorie di **persone fisiche e gruppi verosimilmente interessati dal suo uso** nel contesto specifico;
d) i rischi specifici di danno che possono incidere sulle categorie di persone fisiche o sui gruppi di persone individuati a norma della lettera c), del presente paragrafo tenendo conto delle informazioni trasmesse dal fornitore a norma dell'articolo 13;
e) una descrizione dell'attuazione delle **misure di sorveglianza umana**, secondo **le istruzioni per** l'uso;
f) le **misure da adottare qualora tali rischi si concretizzino**, comprese le disposizioni relative alla governance interna e ai meccanismi di reclamo.

VALUTAZIONE DI IMPATTO SUI DIRITTI FONDAMENTALI

Art. 2 AI Act

Oltre che a una valutazione di conformità dei sistemi di AI, saranno necessarie valutazioni dei diritti simili a quelle previste dal GDPR, come ad esempio, per alcuni tipi predefiniti di sistemi di IA ad alto rischio, una valutazione dell'impatto sui diritti fondamentali che l'uso del sistema può produrre, che viene poi comunicata all'autorità di vigilanza del mercato.

Nel caso in cui sia già stata effettuata una DPIA, la valutazione d'impatto prevista dall'AI Act (FRIA) si integra con la DPIA: Il rapporto tra la FRIA e la DPIA è chiarito dall'AI Act, secondo cui se qualsiasi obbligo relativo alla FRIA è già rispettato in virtù della DPIA effettuata ai sensi del GDPR, la FRIA è richiesta solo per quegli aspetti che non sono già ricompresi nella DPIA

AVVERA

GOVERNANCE DEI DATI

- **Art. 10 AI Act,** è strutturato per promuovere la condivisione sicura ed efficace dei dati tra i vari attori coinvolti nello sviluppo dei modelli IA

- con riferimento ai sistemi di AI ad alto rischio che prevedono l'uso dei dati (anche non personali) per l'addestramento dei modelli di AI, è previsto che i set di dati di addestramento, convalida e test soddisfino specifiche pratiche di governance e criteri di qualità:

- i dati devono essere pertinenti, completi, rappresentativi e privi di errori.

- La governance dei dati è particolarmente rilevante perché riguarda non solo l'accuratezza tecnica e la robustezza dei sistemi IA, ma anche la protezione dei diritti fondamentali degli individui, in particolare in merito alla privacy e alla non discriminazione.

AVVERA

TRASPARENZA E TRACCIABILITÀ

L’ Obbligo di trasparenza (Art. 13) assicura che i **deployer abbiano tutte le informazioni** per utilizzare questi sistemi necessari in modo sicuro e conforme alle normative, e dall'altro, protezione dei diritti umani.

Le istruzioni per l'uso dei sistemi di IA ad alto rischio, debbano essere concise, complete, corrette e chiare, sia in formato digitale che non digitale, assicurando che gli stessi abbiano tutte le informazioni per utilizzare questi sistemi necessari in modo sicuro e conforme alle normative.

Questi obblighi hanno implicazioni significative sui processi aziendali, richiedendo l'implementazione di sistemi di gestione documentale adeguati e la definizione di responsabilità chiare per la tenuta e l'aggiornamento della documentazione.

AVVERA

DOCUMENTAZIONE TECNICA

Predisposta **prima della immissione nel mercato** del sistema e del suo utilizzo e va mantenuta aggiornata per tutto il ciclo di vita del sistema:

1. **Descrizione del sistema di AI** (Scopo previsto e logica generale del sistema; versione del software e data di rilascio);
2. **Descrizione dettagliata dei componenti:** (Architettura del sistema; Algoritmi, modelli di dati e parametri);
3. **Processi di sviluppo:** Metodologia di progettazione e sviluppo; Procedure di controllo e qualità).
4. **Specifiche tecniche:** Specifiche delle prestazioni del sistema; Grado di accuratezza e livelli di qualità e sicurezza);
5. **Dettagli sulla governance dei dati:** Metodi di raccolta, etichettatura e cura dei dati; Protocolli di protezione dei dati);
6. **Sistema di monitoraggio:** Metodi per monitorare, identificare e correggere bias; Procedure per la valutazione continua);
7. **Misure di supervisione umana: (**Dettagli delle misure di controllo; Formazione richiesta per gli operatori umani);
8. **Valutazione del rischio:** (Risultati dettagliati della valutazione del rischio: Misure di mitigazione del rischio);
9. **Conformità: (**Dimostrazione della conformità con i requisiti dell'AI Act; Risultati dei test di conformità);

AVVERA

SORVEGLIANZA UMANA

L'art. 14 si concentra sulla necessità di linee guida per la sorveglianza umana dei sistemi IA ad alto rischio, per garantire garantendo sia che questi siano utilizzati in modo sicuro e conforme alle normative vigenti, sia proteggendo i diritti delle persone coinvolte.

Uno degli aspetti principali della sorveglianza umana è la capacità di **interpretare correttamente l'output del sistema** e, in caso di necessità, **intervenire per correggere o interrompere il funzionamento del sistema stesso.**

Per quanto riguarda le misure di supervisione in contesti specifici, come la sicurezza pubblica o la salute, i sistemi di IA possono richiedere che le decisioni critiche siano verificate da persone fisiche: **gli operatori umani devono essere in grado di comprendere le capacità e i limiti del sistema di IA, riconoscendo potenziali errori o anomalie nel suo funzionamento**.

Questo requisito si collega con l'obbligo di formazione previsto dall'articolo 4.3 del Regolamento.

MISURE DI GESTIONE E SICUREZZA:
ROBUSTEZZA, ACCURATEZZA E CYBERSECURITY

- Questo requisito implica l'adozione di misure tecniche per mitigare specifiche debolezze dei sistemi AI, quali attacchi ai dati di addestramento (es. "data poisoning", "model poisoning"), presenza di "bias" o "allucinazioni" nei dati prodotti, attacchi per sovvertire il modello (es. "prompt injection", "model evasion", "adversarial example").
- Queste misure di sicurezza devono essere adottate dai "Provider" dei sistemi AI e anche dalle aziende "Deployer" per i sistemi AI installati sui propri sistemi IT.

AVVERA

LE REGOLE PER I MODELLI DI AI DIRITTI PER USO GENERALE - GPAI

L’AI Act presta particolare attenzione ai modelli di AI per uso generale (GPAI), come i Large Language Model di uso comune quali **GPT o Claude**.

Per questi sistemi, il regolamento prevede disposizioni specifiche, inclusi obblighi di **conformità al diritto d’autore** e **requisiti di trasparenza sui dati di addestramento.**

La Commissione europea ha anche avviato una consultazione su un codice di buone pratiche per i fornitori di GPAI, che affronterà questioni cruciali come la trasparenza, le norme sul diritto d’autore e la gestione dei rischi.

AVVERA

LE REGOLE PER I SOFTWARE OPEN SOURCE

In linea generale, i sistemi di AI che utilizzano software liberi e open source non sono soggetti all'AI Act.

Tuttavia, l'esenzione non vale per i sistemi di AI open source che rientrano nelle categorie dei sistemi vietati o ad alto rischio, né per quelli che interagiscono direttamente con gli individui o espongono le persone a contenuti generati dall'AI.

I GPAI rilasciati con licenze open source che consentono l'accesso, l'uso, la modifica e la distribuzione del modello, e i cui parametri (inclusi pesi, informazioni sull'architettura e sull'uso del modello) sono resi pubblicamente disponibili, godono di un'esenzione più estesa. Tuttavia, questa si applica solo a due obblighi specifici: la redazione della documentazione tecnica sul modello e la messa a disposizione di certe informazioni ai fornitori di sistemi di AI che intendono integrare il GPAI.

Inoltre, l'esenzione non è disponibile per i GPAI considerati a rischio sistemico.

10

AVVERA | SB Società Benefit

COME MITIGARE IL RISCHIO PER EVITARE SANZIONI

AVVERA SRL SB

AVVERA

I RISCHI DEGLI USI DELL'AI

1. Bias algoritmico e discriminazione

L'IA può replicare – o amplificare – pregiudizi contenuti nei dati di addestramento, generando risultati discriminatori nei confronti di dipendenti, clienti o candidati.

2. Violazioni della normativa sulla privacy (GDPR)

Molti strumenti di IA trattano dati personali. Senza una corretta gestione, si rischiano violazioni gravi del **Regolamento UE 2016/679,** con sanzioni fino a 20 milioni di euro o al 4% del fatturato annuo.

3. Dipendenza da strumenti AI

Rischi per la salute mentale e il benessere professionale derivato dall'utilizzo dei sistemi di AI. Uno dei dibattiti aperti tra sociologi e antropologi è se l'utilizzo vada ad impigrirci e a disimparare a svolgere determinate attività. Es. scrivere e-mail professionali o di pensare in maniera critica.

AVVERA

I RISCHI DEGLI USI DELL'AI

4. Responsabilità legale per decisioni automatizzate

Se un sistema IA prende decisioni che incidono sui diritti delle persone (es. selezione del personale, accesso al credito, valutazione delle performance), l'azienda è chiamata a rispondere – anche in assenza di dolo.

5. Impatti ambientali

Grande quantità di energia e grandi quantità di acqua per far raffreddare i data center in cui i dati vengono localizzati e processati. In particolare la GENAI richiede grande potere computazionale e grandi location per fare lo storage dei dati. Per funzionare bene sono necessarie soluzioni cloud dove i dati vengono localizzati e processati.

6. Lavoro invisibile e Diritti Umani

dietro ai modelli di GENAI c'è un lavoro umano: questi modelli, prima che vengano rilasciati sul mercato, ci sono migliaia di addestratori che fisicamente vanno a verificare che l'output sia accurato e sulla base di questo danno un feedback. Dietro di loro ci sono migliaia di annotatori di dati.

AVVERA

COME MITIGARE I RISCHI?

Adottare un'AI etica e responsabile: Le organizzazioni devono integrare linee guida e una cultura aziendale orientata a responsabilità e inclusività, prevenendo conseguenze negative per individui e società.

4 pilastri:

1. Accountability: essere sicuri che i dati che vengono messi in pasto ai modelli seguono il GDPR;

2. Cybersecurity by design: far sì che questi modelli, non solo in fase di addestramento ma anche in fase di adozione vengono sviluppati in maniera sicura (furti di dati o problemi di cybersecurity);

3. Adozione di questi modelli in sicurezza: dare consapevolezza agli utenti in relazione alle criticità e i reali ambiti di applicazione dell'AI.

4. Formazione e adozione di una governance basata su best practices: costante aggiornamento delle norme etiche e legali per stare al passo con le continue evoluzioni della tecnologia.

AVVERA

COSA FARE PER ESSERE IN REGOLA

1. Accountability: valutazione d'impatto sull'AI (AI Impact Assessment): eseguire una valutazione d'impatto sui diritti fondamentali (obbligo previsto dall'art. 9, 27 AI Act), analizzando:

– La qualità dei dati impiegati.

– I potenziali rischi di discriminazione.

– Le misure adottate per prevenire pregiudizi o esiti ingiustificati.

2. Trasparenza nei confronti degli utenti. È obbligatorio:

– Es. Nel caso di selezione del personale, informare chiaramente i candidati che un algoritmo AI è coinvolto nel processo di selezione.

– Dare la possibilità di chiedere chiarimenti sulle decisioni automatizzate (art. 13 AI Act).

3. Supervisione e intervento umano. Ogni decisione basata su AI deve essere verificabile da un essere umano, che può correggere o revocare l'esito proposto dall'algoritmo (art. 14 AI Act).

AVVERA

BEST PRACTICES

Una strategia per le aziende:

Implementare un sistema di compliance robusto che possa integrare etica, diritto, sicurezza e governance:
La designazione di un responsabile per la conformità all' AI Act;
Sviluppare procedure interne per garantire la conformità continua.

Mappare e classificare:
Mantenere una documentazione completa e aggiornata su tutti gli i tipi di AI e aspetti dei sistemi di AI
Prepararsi a fornire questa documentazione alle autorità se richiesta.

Formazione del personale:
Assicurare che tutto il personale coinvolto nello sviluppo e nell'utilizzo di sistemi di AI sia adeguatamente formato sulle disposizioni dell'AI Act.

AVVERA

BEST PRACTICES

Monitoraggio proattivo:
Implementare sistemi robusti di monitoraggio dopo l'immissione sul mercato;
Sviluppare processi per l'identificazione e la segnalazione tempestiva di incidenti.

Collaborazione con le autorità:
Adottare un approccio collaborativo con le autorità di vigilanza
Considerare la partecipazione a consultazioni pubbliche e iniziative di settore.

Prepararsi alle ispezioni:
Sviluppare protocolli interni per gestire eventuali ispezioni o richieste di informazione da parte delle autorità.

Gestione del rischio:
Incorporare considerazioni relative all'AI Act nella strategia complessiva di gestione del rischio aziendale.

11

AVVERA | SB Società Benefit

APPROCCI PER UNA GESTIONE AGILE ED EFFICACE

AVVERA SRL SB

AVVERA

ROADMAP DI ADEGUAMENTO

I passi da compiere:

- **Implementazione: -** entro febbraio 2025 - dotarsi **di policy relative alle pratiche vietate dall'articolo 5 del Regolamento:** analisi approfondita dei sistemi utilizzati e adozione di misure per evitare l'utilizzo di pratiche considerate inaccettabili, come il social scoring o la manipolazione subliminale.
- **Se utilizzo GPAI**: - entro agosto 2025 - effettuare **audit specifici,** ai sensi dall'art. 55 del Regolamento: competenze tecniche specialistiche e che dovrebbe essere pianificata con largo anticipo.
- **Certificazione**: - entro agosto 2026 - **i sistemi ad alto rischio dovranno essere certificati secondo le procedure previste dal Regolamento:** un percorso di adeguamento graduale e strutturato, con investimenti significativi in termini di risorse umane e tecnologiche.

AVVERA

I PASSI PER UNA COMPLIANCE EFFICACE

Ambito di applicazione

Il primo passo necessario richiede di determinare se la tecnologia oggetto dell'analisi rientra nella definizione di **sistema di IA** (fornita dall'articolo 3(1)) o in quella di **modello di IA per finalità generali** (fornita dall'articolo 3(63)). Come già evidenziato, sono previsti obblighi generali per i sistemi di IA (articoli 8-15 e 50) e obblighi specifici per i modelli di IA per finalità generali (articoli 53-55), in ragione delle difficoltà legate alla supervisione delle molteplici capacità di questi ultimi.

Livello di rischio

Soluzioni come quelle applicate al settore della sanità, dell'istruzione, della giustizia, della sicurezza pubblica, ecc. avranno più probabilità di rientrare nella categoria delle **pratiche proibite** (articolo 5) o in quelle che **pongono un rischio elevato** (sistemi di IA ad alto rischio, *ex* articolo 6, ma anche modelli di IA con finalità generali che pongono un rischio sistemico, *ex* articolo 51).

AVVERA

I PASSI PER UNA COMPLIANCE EFFICACE

Utilizzo

L'analisi degli scopi di utilizzo dell'intelligenza artificiale è necessaria in primo luogo per individuare i casi esclusi *tout-court* dall'ambito di applicazione dell'AI Act. Le norme presenti nel Regolamento non si applicano infatti ai sistemi di intelligenza artificiale utilizzati esclusivamente a fini di ricerca, né a quelli utilizzati per scopi strettamente personali. L'analisi delle finalità legate all'impiego di un sistema di IA è inoltre fondamentale per affinare il risultato già raggiunto con l'individuazione del settore di riferimento, di cui al punto precedente. Per fornire un esempio, diversi sistemi di categorizzazione biometrica possono essere classificati come vietati o ad alto rischio, ma anche a rischio limitato o minimo, a seconda delle specifiche finalità e delle tipologie di informazioni trattate.

Ruolo

Identificare il ruolo che l'operatore riveste all'interno del ciclo di distribuzione del sistema di IA o del modello di IA con finalità generali. L'AI Act prevede infatti obblighi specifici per i fornitori (articoli 16-21, 47, 49 e 50), per i rappresentanti autorizzati (articoli 22 e 49), per gli importatori (articoli 23 e 25), per i distributori (articoli 24 e 25) e infine per i deployer (articoli 25-27 e 50).

AVVERA

I PASSI PER UNA COMPLIANCE EFFICACE

Disposizioni applicate

Individuare la categoria di rischio e il ruolo di appartenenza permette quindi di individuare correttamente la scadenza del “periodo di grazia” e definire una timeline più precisa per l’implementazione degli obblighi previsti, assicurando una compliance già completa nel momento in cui le autorità preposte inizieranno a vigilare sulla corretta applicazione delle misure imposte dal Regolamento.

Integrazione

Il passaggio più complesso è sicuramente quello dell’implementazione degli obblighi previsti, che richiederà - oltre ad un’ottima padronanza del contenuto dell’AI Act - anche un’attenta attività di coordinamento tra il nuovo regolamento e la normativa già esistente. L'AI Act si inserisce infatti panorama legislativo più ampio che include vari strumenti normativi già adottati dall'Unione Europea per garantire lo sviluppo di un mercato unico digitale equo o sicuro. Tra questi si evidenziano, in primo luogo, il Regolamento Generale per la Protezione dei Dati (Regolamento 2016/679/UE), la Direttiva Copyright (Direttiva 2019/790/UE) e la Direttiva sulla responsabilità da prodotto difettoso (adottata in seduta plenaria il 12 marzo 2024, per l’aggiornamento della Direttiva 85/374/CEE.

AVVERA

IMPLEMENTAZIONE DELL' AI IN AZIENDA

Per applicare al Regolamento, le aziende dovranno:

- Definire una **politica aziendale** per la scelta, adozione e gestione dei sistemi AI, individuando ruoli e responsabilità. È fondamentale nominare un responsabile del governo dei sistemi AI
- **Integrazione AI Act e GDPR:** analisi unica e integrata che unisca tutele sui diritti, requisiti tecnici, sorveglianza umana, impatti etici e misure di mitigazione previste da entrambe le normative.
- **Attivare una governance sin dall'inizio:** coinvolgere DPO, CISO, HR, Legal, IT
- **Mappare e classificare:** creare un **catalogo dei sistemi AI utilizzati**, classificandoli in base ai rischi secondo il Regolamento. Per ogni sistema vanno specificate **informazioni come scopo d'uso, dati trattati, valutazione dei rischi**, ecc.
- **Valutare i rischi** di ogni sistema AI secondo i criteri del Regolamento, considerando anche i rischi specifici aziendali legati **al caso d'uso. La valutazione può differire da quella fornita dal fornitore del sistema.** Adottare misure di gestione e sicurezza adeguate ai rischi, in collaborazione con i fornitori IT.

AVVERA

IMPLEMENTAZIONE DELL' AI IN AZIENDA

- Garantire una **supervisione umana significativa:** intervento, umano, tempestivo e consapevole: perché il sistema sia legalmente sostenibile è necessario correggere, bloccare e intervenire.
- **Applicare cybersecurity by design:** audit, trail, controlli d'accesso, monitoraggio continuo, resilienza ai data poisonig: ogni AI è un asset digitale, da trattare come infrastruttura critica.
- **Informare e coinvolgere i lavoratori**: trasparenza radicale: informazioni chiare, accessibili. Formare e sensibilizzare il personale sull'uso corretto dei sistemi AI, attraverso **programmi di informazione e formazione periodici.**
- Costruire l'AI Compliance File: fascicolo tecnico-giuridico completo e aggiornato, che documenti progettazione, test, audit, controlli e misure adottate.
- **Mantenersi aggiornati sulle linee guida che verranno pubblicate dalle autorità** competenti e prevedere un piano di adeguamento strutturato tenendo conto delle ulteriori previsioni dell'AI Act che diventeranno applicabili nel prossimo futuro.

AVVERA

AI POLICY

Una **AI Policy** ben costruita consente di governare l'uso de sistemi di AI in modo responsabile e conforme. Alcuni elementi essenziali:

- Ambiti e limiti di utilizzo dell'IA in azienda (tutela dei dati personali e delle informazioni aziendali riservate)
- Linee guida per il controllo dell'output;
- Ruoli e responsabilità interne (Data Protection Officer, AI Manager, HR, IT, Compliance);
- Le conseguenze derivanti da un uso scorretto delle tecnologie AI (la tutela dei diritti di proprietà intellettuale e del diritto d'autore di terze parti e i profili giuslavoristici);
- La cybersecurity e la gestione degli incidenti;
- Obblighi di formazione e sensibilizzazione per i dipendenti;
- Meccanismi di audit e revisione periodica delle soluzioni IA in uso;
- Gestione della documentazione e del registro dei sistemi IA ad alto rischio, in linea con l'AI Act.

AVVERA

NUOVE DINAMICHE DEL LAVORO

L’implementazione dei sistemi di AI in azienda, se utilizzati in modo consapevole, garantiscono un vantaggio competitivo:

- Nuove opportunità di innovazioni;
- Riduzione tempi di produzione;
- Accelerazione tempi di sviluppo;
- Apertura di nuove possibilità per prodotti, servizi ed esperienze;
- Efficienza e qualità del lavoro in team: supporto tecnologico che facilita e arricchisce le fasi del progetto;
- Maggiore produttività e stimolo della creatività (chiedere nuove idee, vedere un problema da prospettive diverse, simulazione di scenari).

AVVERA

SANDBOX

- Al capo VI del regolamento (UE) 2024/1689 sono disciplinate le **misure a sostegno dell'innovazione** (artt. 57-63). Ambiti e limiti di utilizzo dell'IA in azienda: Ogni Stato Membro è tenuto a istituire almeno un Sandbox entro il **2 agosto 2026**. Possono inoltre essere istituite Sandbox a livello regionale e locale, nonché Sandbox congiunte, co-gestiti con altri Stati membri.
- Questi spazi consentono ai provider di IA di **sviluppare, testare e validare sistemi di IA innovativi** sotto la supervisione delle autorità di sorveglianza del mercato: Le autorità sono tenute a fornire orientamenti ai partecipanti riguardo alle loro aspettative di compliance e a come soddisfare i requisiti previsti dall'AI Act, il che può includere la possibilità di testare il sistema di IA sulla base di condizioni reali.
- Vantaggi per le imprese e per le Autorità - Una volta completata con successo la Sandbox, l'autorità rilascia un rapporto finale ("exit report"), che può essere utilizzato dall'azienda partecipante per dimostrare la conformità alle normative pertinenti, incluso il superamento delle valutazioni di conformità.
- Fra queste, è bene menzionare **l'AI Skills Strategy**, ovvero la strategia che ambisce ad accelerare le iniziative di sviluppo e miglioramento delle competenze IA, e l'**AI Pact**.

AVVERA

A LIVELLO EUROPEO

- EU AI Act Compliance Checker |

REGOLAMENTO EUROPEO SULL'INTELLIGENZA ARTIFICIALE

2024/1689

AI COMPLIANCE:
QUELLO CHE LE AZIENDE DEVONO SAPERE PRIMA DI USARE L'INTELLIGENZA ARTIFICIALE

AVVERA | SB Società Benefit